

NH-1

CONTINUED

EXHIBIT A

US006748541B1

(12) **United States Patent**
Margalit et al.

(10) Patent No.: **US 6,748,541 B1**
(45) Date of Patent: **Jun. 8, 2004**

(54) **USER-COMPUTER INTERACTION METHOD FOR USE BY A POPULATION OF FLEXIBLY CONNECTABLE COMPUTER SYSTEMS**

(75) Inventors: Yanki Margalit, Ramat Gan (IL); Dany Margalit, Ramat Gan (IL)

(73) Assignee: Aladdin Knowledge Systems, Ltd., Tel Aviv (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/412,292

(22) Filed: Oct. 5, 1999

(51) Int. Cl.⁷ G06F 11/30

(52) U.S. Cl. 713/201; 713/161; 713/168; 713/176; 713/183; 713/200

(58) Field of Search 713/201, 161, 713/168, 176, 183, 200

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,343,529 A * 8/1994 Goldfine et al. 705/75
5,371,794 A * 12/1994 Diffie et al. 713/156
5,926,624 A * 7/1999 Katz et al. 709/217
5,941,956 A * 8/1999 Shirakihara et al. 709/245

FOREIGN PATENT DOCUMENTS

DE 19631050 A1 2/1998 H04L/25/20
EP 0 554 164 A1 8/1993 G06K/7/00
EP 0 848 315 A2 6/1998 G06F/1/00
WO 94/10773 5/1994 H04K/1/00

OTHER PUBLICATIONS

P. Gueulle, "Un "dongle" à puce de télécarte," ("A Telephone Card Chip Dongle"), *Electronique Radio Plans*, Nov. 1991, No. 528, pp. 75-78.
"How Does It Work," *Wibu-Key User's Guide*, Version 2.5, pp. 12-16; 25-28; 153-154; and 163-164, Jul. 1998.

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Aladdin Knowledge Systems Announces Software Protection Solutions for Universal Serial Bus Port—USB—HASP & Hardlock—USB," Oct. 15, 1997, 2 pages, http://www.aks.com/press_forum/pr/97oct15.htm.

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Aladdin's USB Software Protection Key Scores 100% in Industry Tests," Dec. 8, 1997, 2 pages, http://www.aks.com/press_forum/pr/97dec8.htm.

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Industry-Leading Software Protection Via the New Universal Serial Bus (USB) Port with Total Transparency and Ease-of-Use," Mar. 2, 1998, 2 pages, http://www.aks.com/press_forum/hasp98/pressusb.htm.

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Aladdin Announces Development of Machasp—USB," May 27, 1998, 2 pages, http://www.aks.com/press_forum/hasp98/macusb.htm.

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Aladdin Launches Machasp USB for Comdex," Nov. 12, 1998, 2 pages, http://www.aks.com/press_forum/hasp98/machaspubs.html.

(List continued on next page.)

Primary Examiner—Thomas R. Peeso

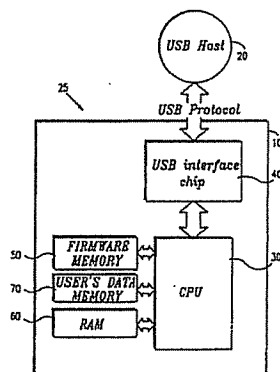
(74) Attorney, Agent, or Firm—Hoffman, Wasson & Gitler, PC

(57)

ABSTRACT

A user-computer interaction method for use by a population of flexibly connectable computer systems and a population of mobile users, the method comprising storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectable computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

11 Claims, 5 Drawing Sheets



US 6,748,541 B1

Page 2

OTHER PUBLICATIONS

Aladdin Knowledge Systems Ltd., Aladdin Press Forum, "Aladdin Announces EToken-Next Generation Security Key Based on Universal Serial Bus Port," Jan. 19, 1999, 3 pages, http://www.aks.com/press_forum/etoken99/etoken.html.
 Rainbow Technologies, Inc. Press Release, "Rainbow Technologies ADDS USB Support for PC and Macintosh Software Developers to Sentinel Line," Nov. 17, 1998, 2 pages, <http://www.rainbow.com/invest/pr98111b.html>.
 Rainbow Technologies, Inc. Press Release, "Rainbow Technologies Announces New Exportable Ikey Universal Serial Bus (USB) Authentication Token," Mar. 15, 1998, 2 pages, <http://www.rainbow.com/invest/pr990315a.html>.
 Rainbow Technologies, Inc. Press Release, "Rainbow Technologies' Ikey Model M2 Now Available with Secure Digital Certificate Storage and 1024-Bit RSA Support," Mar. 15, 1999, 2 pages, <http://www.rainbow.com/invest/pr990315b.html>.

Rainbow Technologies, Inc. Press Release, "Rainbow Today Announced Its New OEM Line of Cryptographic USB Tokens for Virtual Private Networks (VPN)," Jan. 19, 1999, 2 pages, <http://www.rainbow.com/invest/pr990119a.html>.

Universal Serial Bus Specification, Compaq, Intel, Microsoft, NEC, Sep. 23, 1998, Revision 1.1, pp. 1-311.

Materials Collected from the World Wide Web: Press Release, "Gemplus and SCM Microsystems Sign a Development and Manufacturing Agreement," Mar. 25, 1998, 1 page, <http://pluton.gemplus.fr/ns-scarc.../aaaa1768037f23&ns-doc-off>.

Materials Collected from the World Wide Web: "Digital Persona Unveils Fingerprint Recognition System for PCS and Internet," Apr. 19, 1998, 1 page.

* cited by examiner

FIG. 1

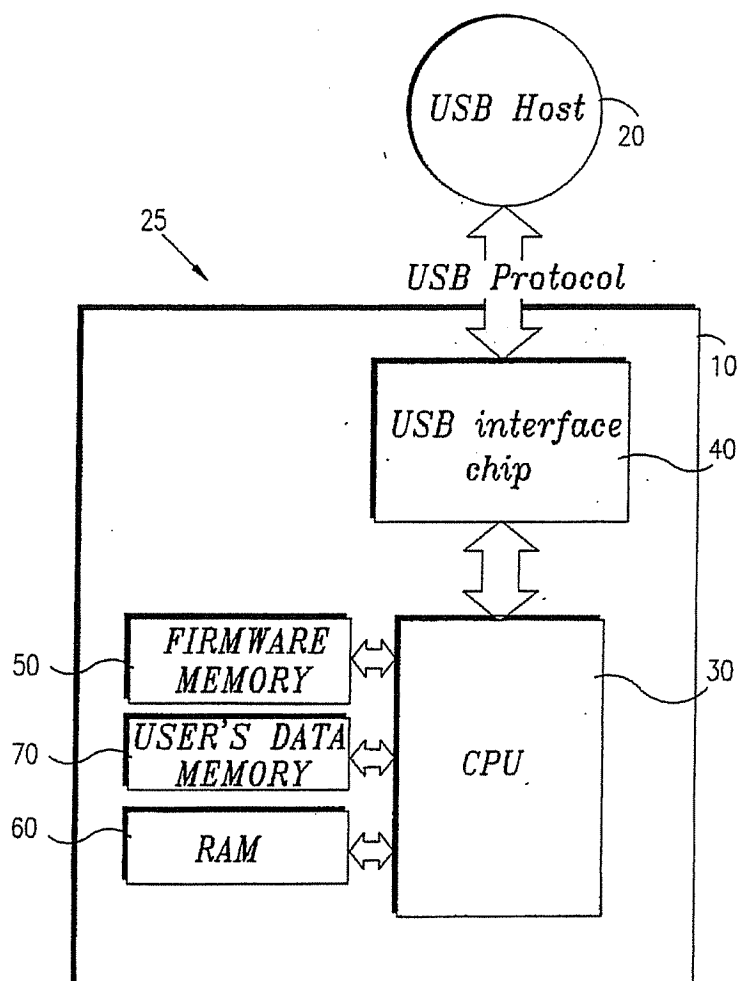


FIG. 2

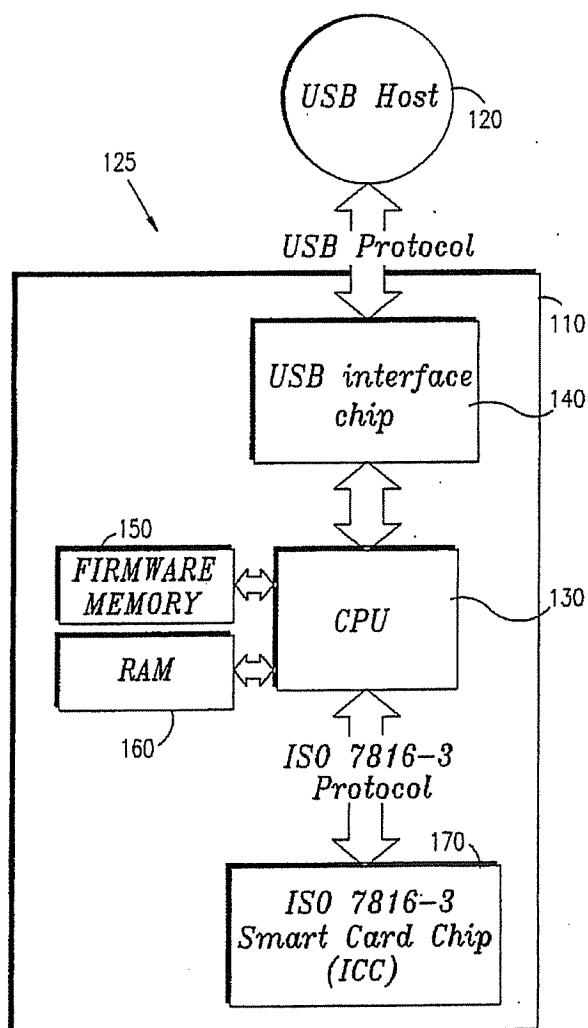


FIG. 3

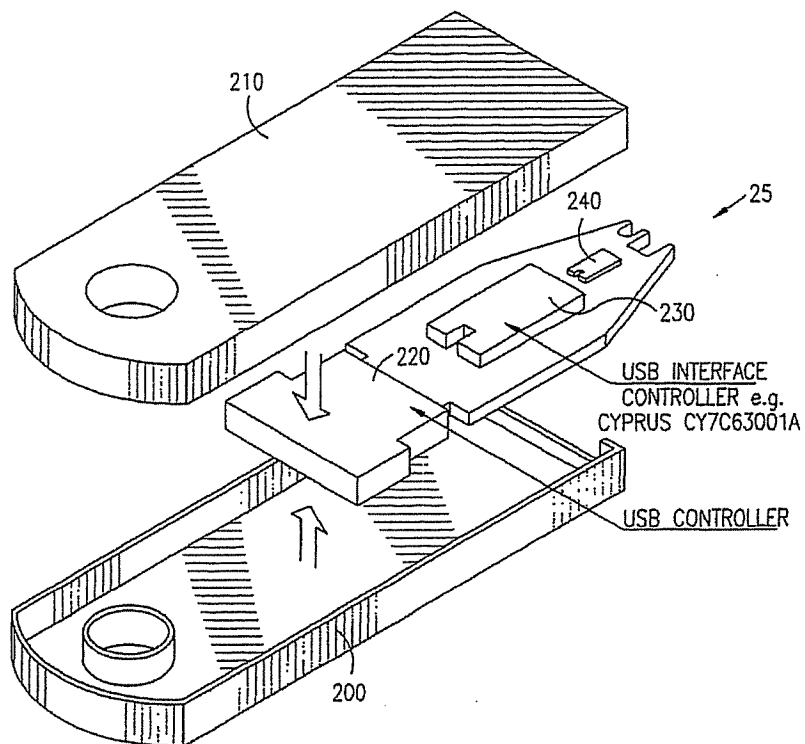
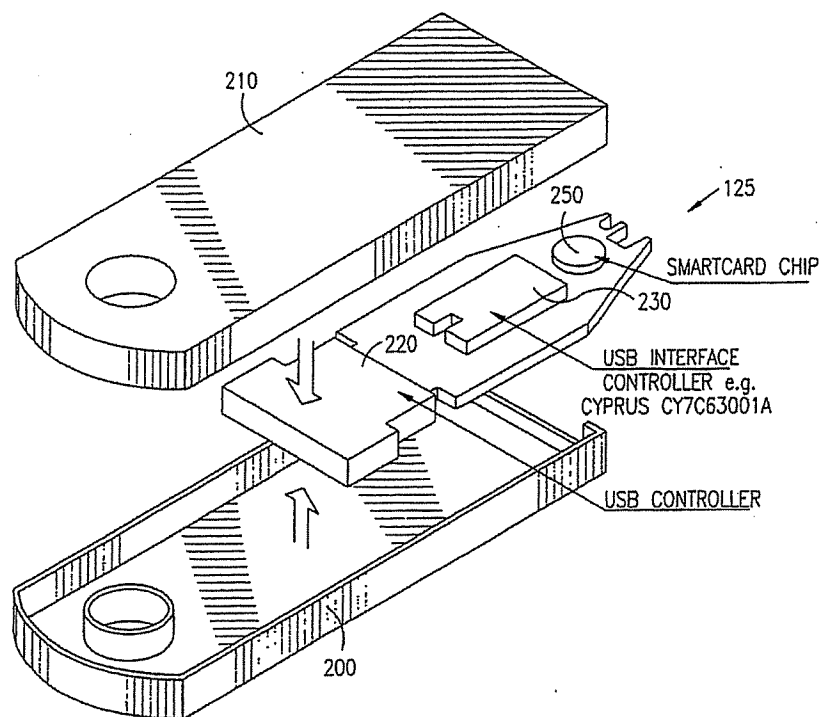


FIG. 4



U.S. Patent

Jun. 8, 2004

Sheet 5 of 5

US 6,748,541 B1

FIG. 5B

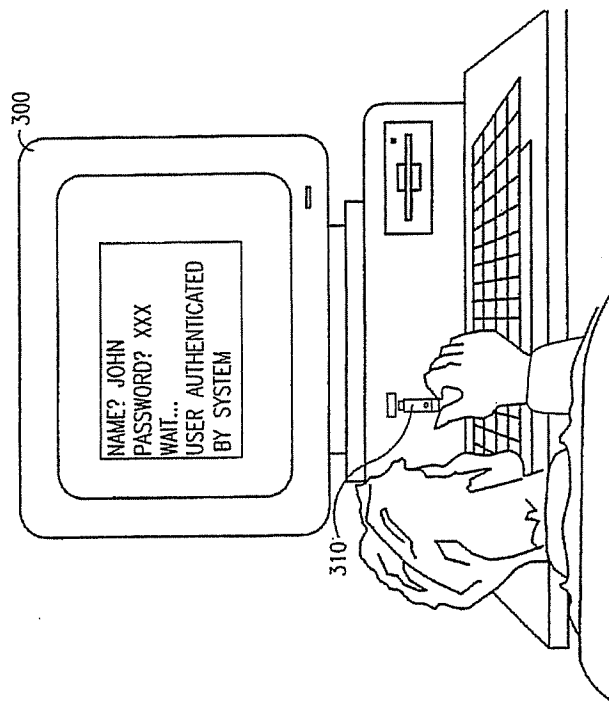
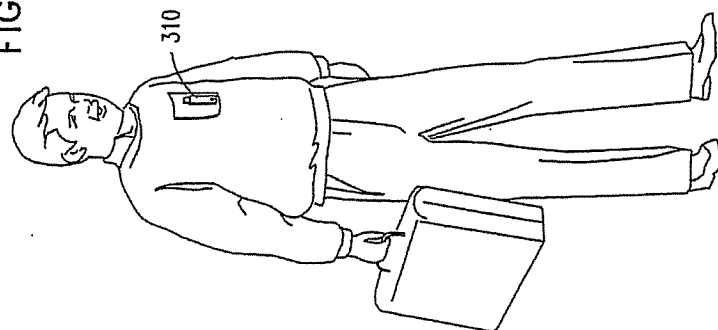


FIG. 5A



US 6,748,541 B1

1

USER-COMPUTER INTERACTION METHOD FOR USE BY A POPULATION OF FLEXIBLY CONNECTABLE COMPUTER SYSTEMS

FIELD OF THE INVENTION

The present invention relates to flexibly connectible computer apparatus and methods for using flexibly connectible hosts.

BACKGROUND OF THE INVENTION

The USB interface is described in specifications available over the Internet at www.usb.org.

Firewire technology, also termed "IEEE 1394 technology", is an alternative to USB which also provides flexible connectivity and is described in the IEEE 1394 standard.

USBHasp is an Aladdin software protection product, announced in October 1997, which includes a USB key. USBHasp does not control access of a user to a computer network but rather impedes interaction between software and a computer system by activating a copy of the software only if a USB key corresponding to that copy is plugged into the computer system.

Conventionally, the only devices which have interacted via USB have been computers, keyboard, monitor, printer, mouse, smart card readers, and biometric readers.

Conventional devices for providing computerized servicing to a mobile or stationary population of users typically include a smart card reader. The members of the mobile population bear smart cards which are used to interact with the computerized servicing device via the smart card reader.

A particular disadvantage of smart cards is that they require a smart card reader which is a relatively costly device. Computer hosts which are equipped with a smart card reader are a small subset of the universe of computer hosts because addition of a smart card reader makes the computer considerably more expensive.

German Patent document DE 19631050 describes an interface converter for a universal serial bus having a module with a processor that changes format and protocol into that of a different bus system.

Rainbow Technologies, Inc., in a news release dated Nov. 17, 1998, announce USB software protection keys which can also be used as authentication or access control devices. A unique ID number is assigned to each USB key, enabling the key to replace or supplement personal passwords. The unique ID of the USB key makes it useful as a notebook computer security device providing theft deterrence. Other uses for the USB keys include Web access control, client token for Virtual Private Network access, replacement for password generator tokens and storage of credentials, certificates and licenses.

In a news release dated Jan. 19, 1999, Rainbow Technologies, Inc. announce a new line of USB tokens for VPNs (virtual private networks) which provides end user client authentication to VPNs and enables operator access to secured network equipment. Features of these tokens include "Internet security small enough to fit on a key-ring" and "personalization for the end user". The tokens allow a user to keep personal information in his or her pocket rather than on a hard drive.

A new "unique per individual" model of its USB based tokens was announced by Rainbow Technologies Inc. on Mar. 15, 1999.

2

The disclosures of all publications mentioned in the specification and of the publications cited therein are hereby incorporated by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved flexibly connectible apparatus and improved methods for using the same.

There is thus provided, in accordance with a preferred embodiment of the present invention, a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

Further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises authentication.

Also provided, in accordance with another preferred embodiment of the present invention, is a FCCS plug device to be borne by a mobile user, the FCCS plug device including a portable device which mates with a flexibly connectible computer system and comprises a memory and information characterizing the mobile user and stored in the memory accessibly to the flexibly connectible computer system.

Also provided, in accordance with another preferred embodiment of the present invention, is a population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices including a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory and information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by the mobile user.

Additionally provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a memory connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the memory is accessibly to the flexibly connectible computer system via the mating element.

Also provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a CPU connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

Further in accordance with a preferred embodiment of the present invention, the FCCS plug device also comprises a CPU connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

Still further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises digital signature verification and/or controlling access to computer networks.

US 6,748,541 B1

3

Further in accordance with a preferred embodiment of the present invention, the information characterizing each mobile user comprises sensitive information not stored in the computer system, thereby to enhance confidentiality.

Also provided, in accordance with another preferred embodiment of the present invention, is a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within the population of mobile users and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

Preferably the apparatus also includes a microprocessor operative to receive the USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage and/or for encryption and/or for authentication and/or for access control.

The term "USB port" refers to a port for connecting peripherals to a computer which is built according to a USB standard as described in USB specifications available over the Internet at www.usb.org.

The term "USB plug" or "USB key" or "USB token" refers to a hardware device whose circuitry interfaces with a USB port to perform various functions.

The term "smart card" refers to a typically plastic card in which is embedded a chip which interacts with a reader, thereby allowing a mobile bearer of the smart card to interact with a machine in which is installed a smart card reader, typically with any of a network of machines of this type.

Also provided in accordance with a preferred embodiment of the present invention is an electronic token, which preferably mates with a flexible connection providing port such as the USB port of any computer system such as a PC, laptop, palmtop or peripheral. The electronic token preferably does not require any additional reading equipment. The token may authenticate information and/or store passwords or electronic certificates in a token which may be the size of a domestic house key.

Preferably, when the token is inserted into a flexible connection providing port, a highly secure "dual factor authentication" process (e.g. "what you have" plus "what you know") takes place in which (a) the electronic token is "read" by the host PCC or network and (b) the user types in his or her personal password for authorization.

Suitable applications for the electronic token include authentication for VPN, extranet and e-commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

FIG. 1 is a simplified block diagram of a USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;

FIG. 2 is a simplified block diagram of a USB plug device including a CPU and a ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;

FIG. 3 is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred

4

embodiment of the present invention and implementing the USB plug device of FIG. 1;

FIG. 4 is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB plug device of FIG. 2; and

FIGS. 5A-5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems and a population of mobile users.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to FIG. 1 which is a simplified block diagram of a flexibly connectible USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention.

A particular feature of the USB plug device of FIG. 1 is that it has data storage capabilities and is thus analogous to a memory smart card.

The USB plug device 10 comprises a PCB 25 which includes a microprocessor or CPU 30 such as a Motorola 6805, Cypress chip or Intel 8051; a USB interface device 40; firmware memory 50 serving the firmware of the microprocessor 30; RAM memory 60 of size sufficient to enable contemplated computations on the part of the microprocessor 30; and user data memory 70 which stores a user's data. Some or all of the USB interface device 40, firmware memory 50 and RAM memory 60 may be within the CPU 30.

The USB interface device 40 and/or the firmware memory 50 may be integrated inside the microprocessor 30.

The firmware memory may be any suitable type of memory such as but not limited to ROM, EPROM, EEPROM or FLASH.

The user data memory 70 typically does not include ISO7816-3 memory and may, for example, comprise any of the following types of memory: I²C, X²C, 2/3 wire bus, FLASH.

As shown, the USB plug device 10 is configured to interact with any USB host 20 such as but not limited to a personal computer or Macintosh having a USB port. Key-host interaction is governed by a USB protocol such as the USB protocol described in the USB specifications available over the Internet at www.usb.org. USB packets pass between the USB host 20 and the USB interface chip 40. Each packet typically includes the following components:

- a. USB header;
- b. Data to be stored/read on the user's data memory 70, plus additional information required by protocols of the memory chip 70, such as but not limited to the address to store/read the data, the length of data to store/read, and CRC checksum information.
- c. USB footer.

The flow of data typically comprises the following flow:

The USB interface chip 40 receives USB packets from the USB host 20, parses the data, and feeds the parsed data to the microprocessor 30. The microprocessor 30 writes the data to, or reads the data from, the firmware memory 50, the RAM 60 or the user's data memory 70, using each memory's protocol.

In read operation, the microprocessor 30 passes the data to the USB interface chip 40 which wraps the data in USB packet format and passes it to the host 20.

US 6,748,541 B1

5

FIG. 2 is a simplified block diagram of a USB plug device, constructed and operative in accordance with a preferred embodiment of the present invention, which is a one-piece smart card reader and smart card chip preferably providing both secured storage and cryptographic capabilities. The USB plug device of FIG. 2 includes both a CPU and a smart card chip (ICC) memory 170, typically a ISO7816 (T=0/1) protocol-based chip communicating with the CPU 130 using an ISO7816-3 protocol. The apparatus of FIG. 2 is similar to the apparatus of FIG. 1 except that no separate user's data memory 70 is provided. The size of the RAM 160 is typically at least 262 bytes in order to support the ISO 7816_3 T=0 or T=1 protocols.

Each packet typically includes the following components:

- a. USB header;
- b. ISO7816-3 T=0/1 protocol packet;
- c. USB footer.

The flow of data in the apparatus of FIG. 2 typically comprises the following flow:

The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120.

A particular advantage of the embodiment of FIG. 2 is that smart card functionality is provided but there is no need for a dedicated reader because the plug 110 is connected directly to a USB socket in the host 120.

The invention shown and described herein is particularly useful for computerized systems serving organizations which process sensitive information such as banks, insurance companies, accountants and other commercial organizations, and professional organizations such as medical or legal organizations.

Conventional computer systems include a computer (comprising a motherboard) and at least one peripherals. The computer has a number of different ports which respectively mate with the ports of the various peripherals. Each port typically can mate with only certain peripherals and not with other peripherals. For example, the keyboard cannot be connected to the computer via the computer's printer port.

In state of the art computer systems, also termed herein "flexibly connectible computer systems", the computer and the peripherals each include at least one identical ports having mating ports on any other computer and any other peripheral such that any peripheral can be selectively connected to any computer or to any other peripheral. Also, a peripheral may be connected to the computer not directly as in conventional systems but rather via another peripheral. There is generally always a port available on one or more connected peripherals in an existing computer system such that another peripheral can generally always be connected to an existing computer system.

One example of a flexibly connectible computer system is a USB (universal standard bus) system in which the computer and each peripheral includes a USB port. Another example of a flexibly connectible computer system is the recently contemplated Firewire system.

A "USB plug" is a portable device which mates with a USB system and, as opposed to peripherals which contain mechanical elements, typically comprises only memory and/or CPU and therefore is typically pocket-size. More generally, a USB plug is an example of a plug which can be plugged into a flexibly connectible computer system (FCCS).

6

The term "FCCS plug" is used herein to refer to a portable device which mates with a flexibly connectible computer system and, as opposed to peripherals which contain mechanical elements, typically comprises only memory and/or CPU and therefore is typically pocket-size. It is appreciated that because each peripheral connected onto a flexibly connectible computer system typically has at least one port, therefore, a flexibly connectible computer system of any configuration typically has at least one vacant port available to interact with an FCCS plug. USB tokens and Rainbow tokens are both examples of FCCS plugs.

Typically, each of the plurality of computer system units (computer and one or more peripherals) forming a computer system has at least two identical female sockets and these are interconnected by means of male-male cables. In this embodiment, the FCCS plug may comprise a male socket. However, it is appreciated that any suitable mating scheme may be employed to mate the computer system units and the FCCS plug of the present invention.

A known use for FCCS plugs is use in conjunction with software having plug-recognizing capability. Aladdin and Rainbow both market software which is operative only if the host computer system in which a particular software copy resides

The Aladdin and Rainbow plugs are not used for authentication.

Computer systems are often used to receive information characterizing a mobile user, who is one of a population of mobile users, and to process this information. Such information may comprise user identity authentication information, banking information, access rights information, etc. Conventionally, this information is stored on a smart card which is borne by the user and is presented to the computer system by him. However this requires the computer system to be equipped with a smart card reader, a special piece of equipment dedicated to reading the smart card.

According to a preferred embodiment of the present invention, information characterizing a mobile user is stored on an FCCS plug. Particular advantages of this embodiment of the present invention is that the information is easily borne by the user, on a pocket-size substrate, that any flexibly connectible computer system of any configuration is typically capable of interacting with the user via the FCCS plug, and that no dedicated equipment is required by the computer in order to carry out the interaction.

Reference is now made to FIG. 3 which is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of FIG. 1. As shown, the FCCS plug of FIG. 3 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside a USB connector 220 and the PCB 25 of FIG. 1. The USB connector 220 may, for example comprise a USB PLUG SMT<ACN-0213> device marketed by Aska Technologies Inc., No. 15, Alley 22, Lane 266, Fu Teh, 1st Rd., Hsi Chih, Taipei Shien, Taiwan. The PCB 25 bears the elements 30, 40, 50, 60 and 70 of FIG. 1. Firmware managing the memory 240 may reside on the USB interface controller 230.

Reference is additionally made to FIG. 4 which is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of FIG. 2. As shown, the FCCS plug of FIG. 4 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside the USB connector 220

US 6,748,541 B1

7

and a PCB 125. The PCB 125 bears the elements 130, 140, 150, 160 and 170 of FIG. 2. Firmware managing the smart card chip 250 may reside on the USB interface controller 230.

Smart card functionalities which are preferably provided by the FCCS plug of the present invention include:

1. Controlling access to computer networks: Smart card or plug has ID information, network authenticates and allows access on that basis. Authentication may be based upon "what you have", "what you are" e.g. biometric information and "what you know" (e.g. password).
2. Digital signatures or certificates for verifying or authenticating the identity of the sender of a document.
3. Storage of confidential information e.g. medical information. A smart card or plug may store confidential information and interact with a network which does not store the confidential information.

FIGS. 5A-5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems 300 and a population of mobile users. Information characterizing each mobile user, e.g. name and ID, is loaded into the memory of an FCCS plug 310 to be borne by that mobile user, typically via a USB interface controller such as unit 230 of FIG. 3.

The plug can then be connected to one of the flexibly connectible computer systems and the information characterizing the mobile user employed to perform at least one computer operation typically comprising a conventional smart card functionality such as authentication.

Features of a preferred embodiment of the present invention are now described:

- a. The need for enhanced user authentication
Authentication is the basis for any information security system. The ability to authenticate local and remote users is a critical issue for any LAN/Intranet, multi-user environment
- b. The need for encryption and confidentiality
Content encryption & confidentiality becomes an important issue for both the corporation and the individual users
- c. The need for password and Sign-On security
Password security and user password management are key issues for network corporate users. Passwords represent the single most important security concern in any computing environment.

There is a need today for hardware-based PC security tokens

Sign-On-Key (SOK) is a hardware-based token that seamlessly integrates with Operating Systems & Applications to provide:
a user authentication key
a basis for encryption system
better Sign-On security and enhanced user password management

Software Security

Authentication—3 Basic Elements

Something you know→Password

Something you have→Sign-On-Key

Something you are→e.g., Bio-metrics

Assumption: Two out of the above three provide "good-enough" security.

Encryption

The need to encrypt data, files, disks and information flow is evident.

An hardware-based token with cryptographic abilities can enhance security and ease-of use.

8

Sign-On—Where are Passwords Used?

Log on to your O/S

Log on to your Network (Local, Remote)

Log on to the Internet/ISP

Log on to protected Web pages

Log on to GroupWare/Communications applications

Log on to other sensitive password-protected applications

MS Office & other protected files

PC Boot protection (Bios Password)

Sign-On—Major Security Risks

The Sign-On Process

The Sign-On-Key is a security hardware token, linked by the user to the required applications. Once installed the Sign-On-Key becomes a part of the log-on process. Sign-On-Key provides the user with many security and other functional benefits.

What Can Sign-On-Key Do For a User?

Sign-On Security

Enhance security & authentication. The Sign-On-Key is required in addition to the user password

Sign-On Simplicity

Simplify log-on process and eliminate the need for a password. The Sign-On-Key replaces the password

Password Automatic Re-verification

Check for Sign-On-Key periodically

Single-Sign-On

One Sign-On-Key replaces several passwords for several applications

Mobility & Remote Computing

Sign-On-Key identifies remote users

Sign-On-Key can be used as a data secure container

Theft deterrent of mobile PCs

General Purpose Security Token

File & data Encryption

Authentication

Certificate Key Holder

Sign-On-Key Various Options

Several hardware devices may operate as Sign-On-Keys:

Sign-On-Key USB—A small key that connects to the new standard USB port. USB ports are becoming the new connectivity standard for PCs and Macintosh

Sign-On-Key SC—A smart card based Sign-On-Key.

Can be used with any standard smart card drive

Sign-On-Key USPs & Advantages

Simple, intuitive, easy to use, attractive token

The key IS the token IS the connector

Low cost

High security

High functionality

Memory inside token

Processing power

Automatic Password Re-verification

Multi token connectivity

The Agents' solution

Sign-On-Key Architecture

Full Blown System.

Sign On Agents

The Sign-On-Agent is a software interface between the Sign-On-Key and the application.

The Sign-On-Boot is a special interface for the PC boot password.

Agents may be provided for:

OS/NetWare—e.g., Windows NT, 95/98, 3x, Novell, Unix

US 6,748,541 B1

9

GroupWare/Mail—e.g., Lotus Notes, Outlook, Eudora, Enterprise Applications—e.g., SAP, Baan, MK, Oracle, Magic

Web Browsers—e.g., Explorer, Navigator

The Most Trivial Agent—Windows NT 5

The most trivial Agent will replace the Windows Login session

By doing so Users may gain

Windows Login Extra security

Windows Login simplification (Sign-On-Key replaces password) 10

Sign-On-Key Web Browser' Agent/System

Sign-On-Key can be used as an authentication token to monitor access to secured web pages 15

Web content providers need to authenticate, manage and provide access to their customers

Sign-On-Key API (SDK)

Sign-On-Key API is the interface level between the Sign-On-Key and 3rd parties' applications. 20

This API may be published and opened for usage by certification providers, security companies and SSO companies.

The Sign-On-Key API will also provide encryption & protected memory storage services 25

Sign-On-Key API may be PKCS #11 based/compatible

The Sign-On Process (No CA)

Installation

User installs Agents for required applications

User defines Sign-On Parameters for each application

User stores Sign-On information in Sign-On-Key 30

Sign-On

Application is started

Application reaches its Sign-On dialog 35

Application communicates with the Sign-On-Key

Sign-On permission is granted based on Sign-On-Key

Sign-On-Key As a Secure Container

In addition to unique Key ID, Sign-On-Key will contain personal protected memory area 40

This memory area can be used for storing sensitive information and Certificates

Application' ID keys like Lotus Notes ID file or PGP keys can be stored in this memory

Doing so—Sign-On-Key can be used to increase mobile computing security. Files IDs are stored in Sign-On-Key instead of disk 45

Sign-On-Key an Encryption Engine & Sign-On-Key Crypt

Sign-On-Key can be used as an encrypting device

An encryption API may be provided, e.g., a 100% smart card compatible Sign-On-Key implementation 50

Sign-On-Key Crypt is a Data/File/Hard disk encryption utility based on Sign-On-Key.

Sign-On-Key Certification Toolkit

SOK may use PKCS #11 and X509 and store certificates and/or digital IDs. 55

Sign-On-Key Comprises:

Sign-On-Key USB Token

HASP

Hardlock

Initial Sign-On-Key functionality (Unique ID, personal protected memory)

Sign-On-Key USB extension cable

Sign-On-Key Smart Card Token

Sign-On-Key API (PKCS #11 compliant)

10

Entrust compatibility/link

Windows NT Agent

Navigator and/or Explorer Agent (S/Mime)

Key Plus Crypt (Beta release)

Secure Screen Saver

Initial marketing package

USB proliferation & Windows 98/NT availability are key issues

In the US, Germany & Israel all new PCs shipped are USB equipped.

Section in Early Development stage.

Security Dynamics, ActivCard & Vasco control the market with 1st generation time-based, one-time password or challenge-based tokens

security vendors will look to expand their market share with second generation integrated smart card offerings which will support cryptography, digital signature storage and processing activity

USB: The Better Connection

Almost unlimited port expansion

No add-in cards for new peripherals

no setting of IRQs, DMAs, etc.

One connection type (plug and port)

variety of peripherals

no more guesswork

simple setup, just plug in and go

USB: The Better Connection

Addresses need for speed, multimedia

12 Mb/s, Asynch (bulk) & Isoch (real time) data

stereo-quality digital audio

high frame-rate video (with compression)

high latency applications (force-feedback)

No power bricks with many new peripherals

USB supplies up to 500 mA

PC User experience is vastly improved

Fewer returns and increased sales potential

It is appreciated that USB is only one example of a flexible connectivity standard and the present invention is not intended to be limited to USB.

It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

What is claimed is:

1. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

65 storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and

US 6,748,541 B1

11

accepting the FCCS plug from the mobile user for direct connection to a port of one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

2. A method according to claim 1 wherein said at least one computer operation comprises authentication.

3. A method according to claim 2 wherein said at least one computer operation comprises controlling access to computer networks.

4. A method according to claim 1 wherein said at least one computer operation comprises digital signature verification.

5. A method according to claim 1 wherein said information characterizing each mobile user comprises sensitive information not stored in said computer system, thereby to enhance confidentiality.

6. An FCCS plug device to be borne by a mobile user, the FCCS plug device comprising:

a portable device which mates with a flexibly connectible computer system and comprises a memory; and

information characterizing the mobile user and stored in said memory accessibly to the flexibly connectible computer system.

7. A population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices comprising:

a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory; and

information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by said mobile user.

12

8. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and

a memory connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the memory is accessible to the flexibly connectible computer system via said mating element.

9. An FCCS plug device according to claim 8 and also comprising a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

10. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and

a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

11. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within said population of mobile users; and

accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

* * * * *

EXHIBIT B



US006763399B2

(12) **United States Patent**
Margalit et al.

(10) **Patent No.:** US 6,763,399 B2
(45) **Date of Patent:** Jul. 13, 2004

(54) **USB KEY APPARATUS FOR INTERACTING WITH A USB HOST VIA A USB PORT**

6,168,077 B1 * 1/2001 Gray et al. 235/375
6,216,230 B1 * 4/2001 Rallis et al. 713/185

(75) **Inventors:** Yanki Margalit, Ramat Gan (IL); Dany Margalit, Ramat Gan (IL); Rami Kastershtien, Tel Aviv (IL)

FOREIGN PATENT DOCUMENTS

EP 0554164 A1 8/1993 G06K7/00
EP 0848315 A2 6/1998 G06F1/00
WO 94/10773 5/1994 H04K1/00

(73) **Assignee:** Aladdin Knowledge Systems, Ltd., Tel Aviv (IL)

OTHER PUBLICATIONS

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 21 days.

P. Guelle, "Un Dongle A Puce De Telecarte" Electronique Radio Plans, Nov. 1991, No. 528, pp 75-78.

Wibu-Key, Users guide version 2.50, Jul. 1998, WIBU-Systems AG pp. 12-16; 25-28; 153-154 & 163-164.

* cited by examiner

(21) **Appl. No.:** 10/126,520

(22) **Filed:** Apr. 22, 2002

(65) **Prior Publication Data**

US 2004/0073726 A1 Apr. 15, 2004

Primary Examiner—Jeffrey Gaffin

Assistant Examiner—Tammara Payton

(74) *Attorney, Agent, or Firm*—Mark M. Friedman

Related U.S. Application Data

(57) **ABSTRACT**

(63) Continuation of application No. 09/189,960, filed on Nov. 10, 1998, now abandoned.

(51) **Int. Cl.**⁷ G06F 1/00; G06F 13/00; H04L 9/10

(52) **U.S. Cl.** 710/13; 710/8; 710/63; 710/103; 713/200; 713/202; 713/185

(58) **Field of Search** 710/8, 13, 63, 710/103; 713/200, 202, 185

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,151,647 A * 11/2000 Sarat 710/301

A smart card—host system that operates without the intermediation of a smart card reader. The smart card—host system comprises a host, which has a USB interface, and a portable device, which provides smart card function(s). The portable device has a smart card chip for performing the smart card function(s); a USB interface for connecting the portable device with the host via USB protocol; and a microprocessor for controlling the transfer of data between the USB interface and the smart card chip, for converting data from a USB format to the format of the smart card chip and for converting data from the format of the smart card chip to a USB format.

27 Claims, 2 Drawing Sheets

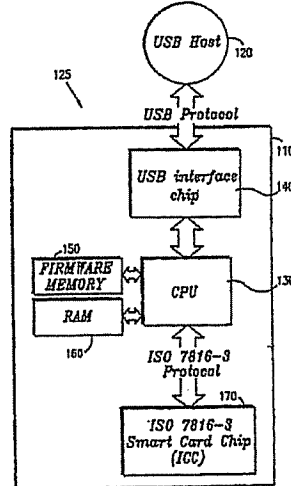


FIG. 1

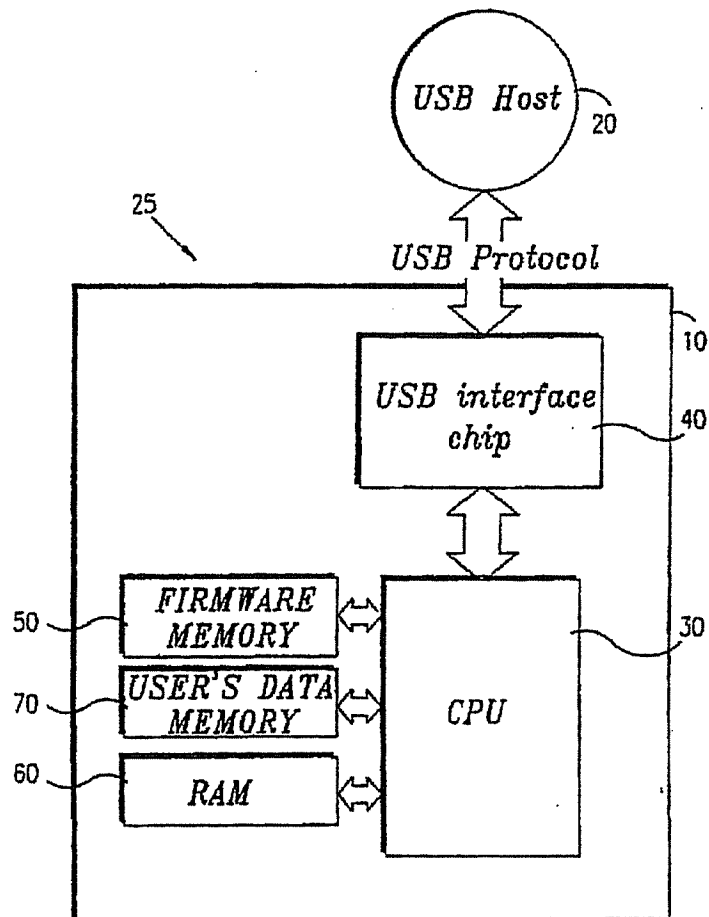
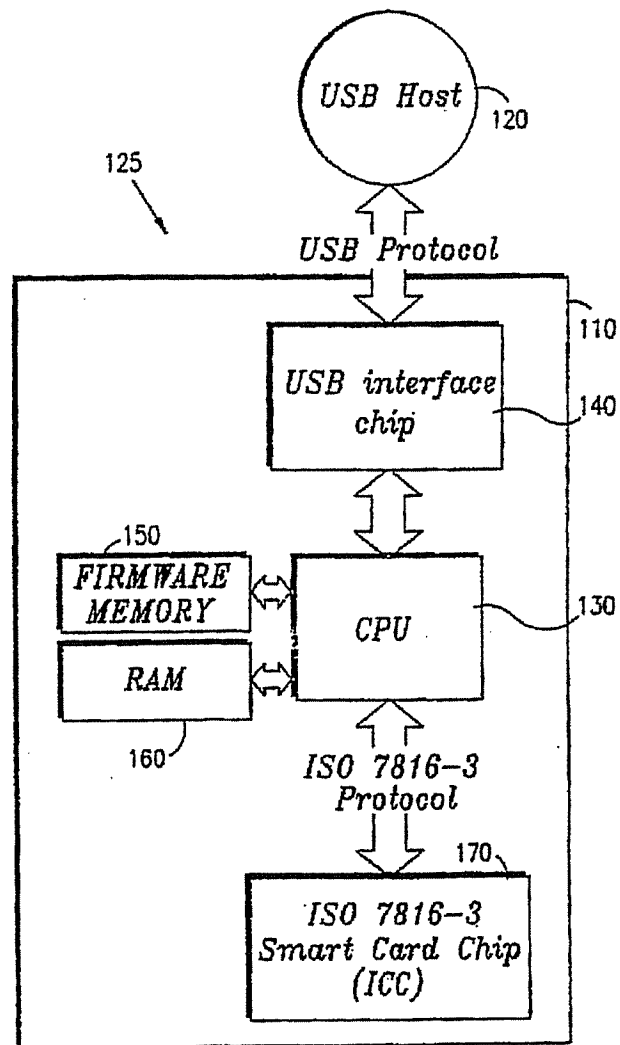


FIG. 2



US 6,763,399 B2

1

USB KEY APPARATUS FOR INTERACTING WITH A USB HOST VIA A USB PORT

The present application is a Continuation application based on the parent patent application 09/189/960 filed Nov. 10, 1998 now abandoned.

FIELD OF THE INVENTION

The present invention relates to USB (Universal serial bus) apparatus and methods for using USB hosts.

BACKGROUND OF THE INVENTION

The USB interface is described in specifications available over the Internet at www.usb.org.

Conventional devices for providing computerized servicing to a mobile or stationary population of users typically include a smart card reader. The members of the mobile population bear smart cards which are used to interact with the computerized servicing device via the smart card reader.

A particular disadvantage of smart cards is that they require a smart card reader which is a relatively costly device. Computer hosts which are equipped with a smart card reader are a small subset of the universe of computer hosts because addition of a smart card reader makes the computer considerably more expensive.

German Patent document DE 19631050 describes an interface converter for a universal serial bus having a module with processor that changes format and protocol into that of a different bus system.

The disclosures of all publications mentioned in the specification and of the publications cited therein are hereby incorporated by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved USB apparatus and improved methods for using the same.

There is thus provided, in accordance with a preferred embodiment of the present invention, USB key apparatus for interacting with a USB host via a USB port, the USB key apparatus including a portable device configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host, a protocol translator operative to translate the USB communications from USB protocol, into smart card protocol such as an ISO7816 protocol, and from smart card protocol into USB protocol and a smart card chip operative to perform at least one smart card function such as authentication, encryption, access control and secure memory.

Also provided, in accordance with another preferred embodiment of the present invention, is USB key apparatus with data storage capabilities, the USB key apparatus including a portable device such as a PCB, configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host and a data storage unit storing information derived from the USB communications.

Preferably the apparatus also includes a microprocessor operative to receive said USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage and/or for encryption and/or for authentication and/or for access control.

The term "USB port" refers to a port for connecting peripherals to a computer which is built according to a USB

2

standard as described in USB specifications available over the Internet at www.usb.org.

The term "USB key" or "USB token" refers to a hardware device whose circuitry interfaces with a USB port to perform various functions.

The term "smart card" refers to a typically plastic card in which is embedded a chip which interacts with a reader, thereby allowing a mobile bearer of the smart card to interact with a machine in which is installed a smart card reader, typically with any of a network of machines of this type.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

FIG. 1 is a simplified block diagram of a USB key device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention; and

FIG. 2 is a simplified block diagram of a USB key device including a CPU and a ISO7816 memory, the USB device constructed and operative in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to FIG. 1 which is a simplified block diagram of a USB key device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention.

A particular feature of the USB key device of FIG. 1 is that it has data storage capabilities and is thus analogous to a memory card.

The USB key device 10 comprises a PCB 25 which includes a microprocessor or CPU 30 such as a Motorola 6805, Cypress chip or Intel 8051; a USB interface device 40; firmware memory 50 serving the firmware of the microprocessor 30; RAM memory 60 of size sufficient to enable contemplated computations on the part of the microprocessor 30; and user data memory 70 which stores a user's data. Some or all of the USB interface device 40, firmware memory 50 and RAM memory 60 may be within the CPU 30.

The USB interface device 40 and/or the firmware memory 50 may be integrated inside the microprocessor 30.

The firmware memory may be any suitable type of memory such as but not limited to ROM, EPROM, EEPROM or FLASH.

The user data memory 70 typically does not include ISO7816-3 memory and may, for example, comprise any of the following types of memory: I²C, XI²C, ¼ wire bus, FLASH.

As shown, the USB key device 10 is configured to interact with any USB host 20 such as but not limited to a personal computer or Macintosh having a USB port. Key-host interaction is governed by a USB protocol such as the USB protocol described in the USB specifications available over the Internet at www.usb.org. USB packets pass between the USB host 20 and the USB interface chip 40. Each packet typically includes the following components:

- a. USB header;
- b. Data to be stored/read on the user's data memory 70, plus additional information required by protocols of the

US 6,763,399 B2

3

memory chip 70, such as but not limited to the address to store/read the data, the length of data to store/read, and CRC checksum information.

c. USB footer.

The flow of data typically comprises the following flow: The USB interface chip 40 receives USB packets from the USB host 20, parses the data, and feeds the parsed data to the microprocessor 30. The microprocessor 30 writes the data to, or reads the data from, the firmware memory 50, the RAM 60 or the user's data memory 70, using each memory's protocol.

In read operation, the microprocessor 30 passes the data to the USB interface chip 40 which wraps the data in USB packet format and passes it to the host 20.

FIG. 2 is a simplified block diagram of a USB key device, constructed and operative in accordance with a preferred embodiment of the present invention, which is a one-piece smart card reader and smart card chip preferably providing both secured storage and cryptographic capabilities. The USB key device of FIG. 2 includes both a CPU and a smart card chip (ICC) memory 170, typically a ISO7816 (T=0/1) protocol-based chip communicating with the CPU 130 using an ISO7816-3 protocol. The apparatus of FIG. 2 is similar to the apparatus of FIG. 1 except that no separate user's data memory 70 is provided. The size of the RAM 160 is typically at least 262 bytes in order to support the ISO 7816_3 T=0 or T=1 protocols.

Each packet typically includes the following components:

- a. USB header;
- b. ISO7816-3 T=0/1 protocol packet;
- c. USB footer.

The flow of data in the apparatus of FIG. 2 typically comprises the following flow:

The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120.

A particular advantage of the embodiment of FIG. 2 is that smart card functionality is provided but there is no need for a dedicated reader because the key 110 is connected directly to a USB socket in the host 120.

The invention shown and described herein is particularly useful for computerized systems serving organizations which process sensitive information such as banks, insurance companies, accountants and other commercial organizations, and professional organizations such as medical or legal organizations.

It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow.

4

What is claimed is:

1. A smart card—host system, wherein a portable device communicates directly with a USB interface of a host, said smart card—host system comprising:

a host, having thereon a USB interface;

a portable device, for providing smart card function(s), said portable device having thereon a smart card chip, for performing said smart card function(s), a USB interface, for connecting said portable device with said host via USB protocol; and a microprocessor, for enabling at least one function selected from the group consisting of controlling the transfer of data between said USB interface and said smart card chip, for converting data from a USB format to the format of said smart card chip and for converting data from the format of said smart card chip to a USB format.

2. A system according to claim 1, wherein said portable device consists of at least one substrate having thereon said smart chip, said USB interface, and said microprocessor.

3. A system according to claim 1, wherein said portable device is a USB key operative as a component into which said smart card chip, said USB interface, and said microprocessor are placed.

4. A system according to claim 1, wherein said portable device further comprises data storage means for at least one function selected from the group consisting of storing data required for the operation of said microprocessor and storing data required for the operation of said smart card chip.

5. A system according to claim 1, wherein said portable device further comprises secured memory.

6. A system according to claim 1, wherein said system is operative to perform at least one function selected from the group consisting of cryptography, authentication, encryption, public key infrastructure, digital signature, RSA and access control.

7. A system according to claim 1, wherein said supports ISO7816 standard.

8. A portable smart card apparatus for providing smart card function(s) to a host system, by communicating directly with a USB interface of the host system, said smart card apparatus comprising:

a smart card chip, for performing said smart card function(s);

a USB interface, for connecting the portable device apparatus with the host system, via USB protocol; and

a microprocessor, for enabling at least one function selected from the group consisting of controlling the transfer of data between said USB interface and said smart card chip, converting data from a USB format to the format of said smart card chip and converting data from the format of said smart card chip to a USB format.

9. An apparatus according to claim 8, wherein said portable device consists of at least one substrate having thereon said smart chip, said USB interface, and said microprocessor.

10. An apparatus according to claim 8, wherein said portable device is a USB key operative as a component into which said smart card chip, said USB interface, and said microprocessor are placed.

11. An apparatus according to claim 8, wherein said portable device further comprises data storage means, for storing data required for the operation of at least one element selected from the group consisting of said microprocessor and said smart card chip.

12. An apparatus according to claim 8, wherein said portable device further comprises secured memory.

US 6,763,399 B2

5

13. An apparatus according to claim 8, wherein said apparatus is operative to perform at least one function selected from the group consisting of cryptography, authentication, encryption, public key infrastructure, digital signature, RSA and access control.

14. An apparatus according to claim 8, wherein said apparatus supports ISO7816 standard.

15. A method for interacting directly between a smart card chip and a host via a USB interface of the host, comprising the steps of:

coupling the host with a USB interface, for interacting with an external device via USB protocol;

providing a portable external device, for being used as a platform for said smart card chip, said portable device having thereon a USB interface, for interacting with the host via USB protocol; and a microprocessor, for executing at least one function selected from the group consisting of controlling the transfer of data between said USB interface and said smart card chip, converting data from a USB format to the format of said smart card chip and converting data from the format of said smart card chip to a USB format;

upon receiving data in the USB interface of said portable device, converting said data from a USB format of said smart card by said microprocessor, and conveying the converted data to said smart card chip; and

upon sending data from said smart card chip to the host, converting said data from the format of said smart card chip to said USB format by said microprocessor, conveying the converted data to said USB interface of said portable device, and there from to the host, via the host's USB interface.

16. A method according to claim 15, wherein said portable device consists of at least one substrate having thereon said smart chip, said USB interface, and said microprocessor.

17. A method according to claim 15, wherein said portable device is a USB key operative as a component into which

6

said smart card chip, said USB interface, and said microprocessor are placed.

18. A method according to claim 15, wherein said portable device further comprises data storage means, for storing data required for operating at least one component selected from the group consisting of microprocessors and smart card chips.

19. A method according to claim 15, wherein said portable device further comprises secured memory.

20. A method according to claim 15, wherein said method is operative to perform at least one function selected from the group consisting of cryptography, authentication, encryption, public key infrastructure, digital signature, RSA and access control.

21. A method according to claim 15, wherein said portable device supports ISO7816 standard.

22. A system according to claim 1, wherein said smart chip is operationally connected directly to said microprocessor.

23. A system according to claim 22, wherein said smart chip is operationally connected directly to said microprocessor on a common substrate.

24. An apparatus according to claim 8, wherein said smart chip is operationally connected directly to said microprocessor.

25. A system according to claim 24, wherein said smart chip is operationally connected directly to said microprocessor on a common substrate.

26. A method according to claim 15, wherein said smart chip is operationally connected directly to said microprocessor.

27. A system according to claim 26, wherein said smart chip is operationally connected directly to said microprocessor on a common substrate.

* * * * *

7

EXHIBIT C

30/04/98

003

HASP - Distribution Contract

This Contract is entered into in Tel-Aviv, Israel, this 1st day of May, 1997, by and between:

Aladdin Knowledge Systems Ltd.

An Israeli corporation, whose principal place of business address is: 15 Beit-Oved Street, Tel-Aviv, Israel, and whose mailing address is: P.O.B. 11141, Tel-Aviv 61110, Israel (hereinafter referred to as "Company"); and:

Feitian Co.

A Chinese corporation, organized and existing under the laws of People's Republic of China, whose principal place of business and mailing address is Haidian Office Bldg. A RM202, No. 11 Haidiannan Rd. Haidian District, P.O.Box 2726, Beijing 100080, China (hereinafter referred to as "Distributor").

WITNESSETH

WHEREAS the Distributor desires to be granted a non-exclusive, non-transferable, right to distribute and market the Product in the Territory;

AND WHEREAS the Company wishes, through the Distributor, to facilitate the marketing and distribution of the Product in the Territory;

NOW THEREFORE, in consideration of the foregoing premises and contracts hereinafter contained, the parties mutually agree as follows:

Article I - Definitions:

In this Contract ("this Contract") and the Schedules attached hereto where the context so admits, words in the singular shall include the plural and vice versa. Words and expressions defined below shall have the following respective meanings:

- 1.1 "The Product/s": Computer hardware and software devices, known as HASP and CODESAFE, the function of which is to prevent unauthorized use of software, and any revisions and/or improvements of the devices provided by Company, and all programming and related documentation, all object code, operator instructions in both hard copy and electronic form, including any other documents necessary and/or related to the use or application of the Product and or any derivatives.
- 1.2 "The Documentation": Any and all documentation necessary and/or related to the use of the Product, in hard copy and/or electronic form.
- 1.3 "The Hardware": All tangible elements in the Product.
- 1.4 "Product Code/s": A unique electronic code, burnt by Company into the Product, that is being used by Customer to protect its software. The Product Code identification is printed on every

- 1.5 "Purchase Price/s": Prices of Products listed in the "Price List".

as Annex C to this Contract. ~~... of the Distributor Price Lists~~ attached hereto.

- 1.6 "Customer": Software developers and/or any other customers in the Territory which will be granted the License or which shall apply for the Product.
- 1.7 "The Territory": North Eastern Provinces of People's Republic of China (North of the Yellow River), but also including Shaanxi Province south of the Yellow River..
- 1.8 "The License": The license granted to the Customer under the License Contract.
- 1.9 "The License Contract": The "ALADDIN KNOWLEDGE SYSTEMS LTD HASP LICENSE AGREEMENT" - attached hereto as Annex B to this Contract.
- 1.10 "Intellectual Property Rights": The right, title and interest in and to any and all trademarks and trade-names, patents, copyrights, which have or which may be registered in the future, and all the know-how regarding the Product, and any part thereof, including the Customers list.

Article II - Appointment

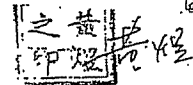
- 2.1 Subject to the terms and conditions set forth in this Contract, the Company hereby grants to the Distributor and the Distributor hereby accepts, a non-exclusive, non-transferable, right to market and distribute the Product.
- 2.2 The foregoing right is limited solely to the Territory.
- 2.3 Company is entitled, upon its sole discretion, to appoint other distributor/s, agent/s, representative/s in the Territory; and/or to establish a branch or affiliated entity which would distribute the Product in the Territory; and/or to distribute the Product in the Territory and to sell or license the Product, directly or indirectly, to Customers in the Territory.

Article III - Title & Ownership

- 3.1 The Distributor acknowledges that the Software and all programming and related Documentation, all object code, design documents, operator instruction in both hard copy and electronic form, including any other documents necessary and/or related to the use or application of the Product and or any derivatives, are, and will remain, the property of the Company.
- 3.2 Subject to any rights deriving from any patent (either registered and/or pending and/or that can be registered) the Company and/or any third party holds or shall hold in the Hardware or any part thereof, Distributor shall purchase the Hardware from the Company.
- 3.3 The Distributor acknowledges the Company's exclusive right to the Intellectual Property Rights and it is agreed that all Intellectual Property Rights concerning the Product will be the sole property of the Company.

Article IV - Company, Distributor, Customer

- 4.1 Subject to the terms and conditions set forth in this Contract, Distributor has the right to order the Product from the Company and to facilitate direct distribution of the Product from the Distributor to the Customer in the Territory.



- 4.2 The Distributor will not acquire any right and/or title in the Software and Documentation; and therefore the Customer's License to use the Software will be granted by Company.
- 4.3 To enable the grant of the License, The Distributor shall distribute the Product with a copy of the "ALADDIN KNOWLEDGE SYSTEMS LTD HASP LICENSE AGREEMENT" (i.e. the License Contract).

Article V - Marketing & Service

Marketing:

- 5.1 The Distributor shall devote its best efforts to promote, sell and service the Product to Customers within the Territory. This promotion shall include advertising the Product in relevant magazines and exhibiting the Product in at least one professional trade shows per year.
- 5.2 Company, under its full and absolute discretion, and for the price set by Company, shall furnish Distributor with an initial quantity of catalogue sheets, price lists, technical data, answers to technical and related inquiries originating in the Territory, and any other information which Company shall find reasonably required for distributing the Products in the Territory.
- The Distributor shall pay Company the said price and it will be authorized to translate, on its own initiative and on its own expense, all such literature into other languages for the purpose of alleviating the marketing of the Products.
- 5.3 Company undertakes to assist Distributor in learning the Products. The Distributor should attend:- traveling and stay expenses on Distributors own expense:- an "HASP Technical and Marketing seminar" to be held at the Company's premises, at least once every two (2) years. The first such seminar should take place within three (3) months of the commencement of this Contract.
- 5.4 Distributor undertakes to employ at least one (1) full-time salesperson/s who has experience in marketing the Products and are dedicated to the marketing of the Products.
- 5.5 All advertisements for the Product shall include the words: "An Aladdin Knowledge Systems Ltd. Product" in the language of the advertisement. The Distributor's name or logo should appear with the words: "Distributed By" in the language of the advertisement.
- Distributor shall submit to Company for Company's prior written approval any and all material which the Distributor intends to use for the purpose of promoting the Products if such materials contain information or statements differing from those contained in Company's promotional materials or from The License Contract.
- 5.6 The Distributor shall refrain from seeking Customers or soliciting, directly or indirectly, orders for the Product from outside the Territory or pursuing any active sales' policy of the Product outside the Territory.

Service:

- 5.7 Distributor shall provide a service organization capable of assuming responsibility for the installation, maintenance and support of the Products in accordance with Company's then prevailing Postsales, Training and Service Policies.

- 5.8 Company shall provide Distributor with updates, new releases and new documentation of the Products whenever they become available.
- 5.9 Distributor will employ at least one (1) full time technical support person/s who will be familiar with the Products in depth.
- 5.10 Distributor shall maintain a stock of the Product to satisfy orders from Customers.

Article VI - Parties Obligations

- 6.1 Company shall, 'unless excused' by circumstances beyond the Company's control (in accordance with article 8.4 hereof), promptly send to the Distributor those Products for which the Distributor places orders.
- 6.2 In the event the Company shall sell Products directly to customers within the Territory and shall be actively assisted by the Distributor for that purpose, the Company shall pay the Distributor a royalty fee of 7.5% of the revenue received by the Company from such a sale.
- 6.3 Distributor shall keep the Company - at the Company's request - updated about Customers and provide the Company, every three (3) months, with a list of all the Product's Customers' details, and Customer's Products Codes.
- 6.4 Distributor shall refrain from supplying Products with the same code to different customers.
- 6.5 Distributor agrees and represents that it will refrain from engaging, directly or indirectly, in the distribution, sale and/or service of products which compete, directly or indirectly, with the Product, or any part thereof, while this Contract is in effect and for the period of one year after the termination of the Contract.

The Distributor acknowledges that these restrictions are fair and reasonably required to protect the interest of the Company under this Contract and that these restrictions will not deprive the Distributor of an opportunity to earn a living or to produce a profit.

The Distributor acknowledges and agrees that any breach of the foregoing covenant not to compete will deprive the Company substantially of the consideration for the Company's entering into this Contract and that the amount of injury would be impossible or difficult to fully ascertain. The Company shall, therefore, be entitled to obtain an injunction restraining any violation, further violation or threatened violation of the covenant not to compete set forth above, in addition to any other remedies which the Company may pursue.

The period of time, geographical area and scope of restrictions on the Distributor's activities are intended to be divisible, so that if any provision of such covenant not to compete is found invalid, that provision shall be automatically modified to the extent necessary to make it valid, rather than such provision being declared invalid or void for such reason.

Article VII - Limited Warranty & Limitation Of Liability

- 7.1 Company warrants that (a) the Software will perform substantially in accordance with the accompanying Documentation for a period of ninety (90) days from the date of receipt and (b) that the Hardware under normal use and service, is free from defects in materials and workmanship for a period of twelve (12) months of the date of receipt. Any implied

workmanship for a period of twelve (12) months of the date of receipt. Any implied

warranties on the Software and Hardware are limited to ninety (90) days and twelve (12) months, respectively.

- 7.2 Company shall supply, at its expense, within twelve (12) months from the day of delivery by the Company, units of the Product to be exchanged with any units found to be faulty in workmanship or materials and sent back to the Company.

Distributor will notify Company, in writing, of such damage or defect within 10 working days of receipt. Company will send a replacement for the Products 10 working days after such notification.

This Limited Warranty is void if failure of the Software or defective Hardware has resulted from: (i) accident, abuse or misapplication and/or modifications are made to the Product by any one other than Company; (ii) attachments, features or devices which are employed on the Hardware which are not supplied by Company or not approved for use, in writing, by Company; (iii) Software other than the current version of the Software available from Company is used on the Hardware. The warranty and remedies set forth herein are exclusive and in lieu of all others, oral or written, express or implied.

- 7.3 Except for and to the extent expressly provided herein, Company makes no warranty or representation, either expressed or implied, with respect to the Product, including its quality, performance, merchantability or fitness for a particular purpose.
- 7.4 The Distributor understands and agrees that the Software is inherently complex and may not be completely free of errors. To the maximum extent permitted by applicable law in no event shall Company be liable for direct, indirect, special, incidental, cover or consequential or any other damage whatsoever (including without limitation damages for loss of business

information or other pecuniary loss) arising out of or related to this Contract or the performance or breach of Company's liability and/or the use or inability to use the Product, even if Company has been advised of the possibility of such damages. In no case shall Company's liability under any provision of this Contract exceed the amount actually paid by Distributor for a Product unit.

- 7.5 Without derogating from the generality of article 4.3 Distributor shall include the provisions stated in this article in any contract and/or other method in which the Distributor shall establish and/or define its business relation with the Customer.

Article VIII - Orders, Prices, Terms of Payment & Delivery

- 8.1 Upon signing this Contract, the Distributor shall place an initial order of at seven hundred (700) Product units.

During the first twelve (12) months after the signing of this Contract, the Distributor shall order at least another three thousand (3,000) units of the Product.

- 8.2 Prices and Terms of Payment:

- (a) For the Products listed on the "Distributor Price List", the Company shall charge the Distributor the prices indicated therein. From time to time the Company may change the Purchase Price for its products and shall give the Distributor written notice of any change of the Purchase Price.

- (b) The Purchase Prices are exclusive of any taxes which, if they exist, shall be paid by the Distributor, and do not include shipping, domestic or foreign duties, or any other charges required in the country of destination.

- (c) Payment for the Products shall be with the order made by the Distributor.

- 8.3 Orders & Delivery:

- (a) The Distributor shall submit all orders for the Product by writing or by telefax.

- (b) For orders up to 1,000 (one thousand) Product units - the Company shall supply the units within 45 (forty five) days of payment. The date of delivery for orders of over the said number of units of the Product shall be agreed upon by both parties for each individual order.

- (c) Shipment of all Products will be Ex-factory Company's plant. The Company's obligation to deliver the Products shall be completely discharged, and all risk of loss or damage shall immediately pass to the Distributor, when the order is transferred to a carrier in Israel. The Distributor shall have the responsibility, with the Company's cooperation, for dealing with the carrier in the event of carrier's misdelivery, loss or damage to the Product.

- 8.4 The Company shall not be liable for any failure to manufacture or for any delay in delivery of the Product due to causes beyond the Company's control. Without derogating from the generality of the above, "causes beyond the Company's control" would include: natural disaster, fire, embargo, strike, failure to secure materials from the usual sources of supply, war, act of government, or any other circumstances beyond the Company's control. The Company shall, however, promptly make delivery when any such cause interfering with delivery shall have been removed.

Article IX - Confidentiality & Intellectual Property Rights

Without derogating from the generality of article 3, and in addition to the Distributor's remaining representations and undertakings in the terms of this Contract, and in consideration of the right given in this Contract, the Distributor hereby represents and undertakes that:

- 9.1 Any proprietary trademarks, trade names, service marks, commercial symbols and/or logos which have been developed, or will be developed in the future, for the Product shall be and remain the sole and exclusive property of the Company.

The Distributor acknowledges and agrees that it has not, does not, and shall not acquire any rights with respect to any such trade-names, trademarks, service marks, commercial symbols and/or logos as a result of the Distributor's use thereof in connection with the Product, and that the Company shall be free, at all times, to use any such trade-names, trademarks, service marks, commercial symbols and/or logos in connection with any other product of services.

- 9.2 In order to protect the Company's patent, copyright and other ownership interests in the Product, the Distributor agrees that as a condition of its rights hereunder, the Product shall contain the same proprietary notices which appear on or in the Product delivered by the Company to the Distributor and as otherwise reasonably required by the Company. More specifically, the Distributor agrees, where applicable, that a valid Company copyright and/or patent notice for the Product will appear on the media for the Product and any consumer

之
印
000

packaging materials associated therein, on any documentation and promotion material for the Product.

It is further agreed that the Distributor must pack and/or ship the Product according to the Company's instructions. Specifically, the Distributor must pack and/or ship Developer's Kits of the Product in a sealed, shrink-wrapped covering. It is further agreed that the Distributor must pack and/or ship any and all software related to the Product in an envelope, sealed with the Company's software license label.

- 9.3 The Distributor shall not, in any manner, represent that it possesses any proprietary interest in the Intellectual Property Rights or the registration thereof, and shall not, directly or indirectly, take any action to contest these Intellectual Property Rights or infringe them in any way.

The Distributor shall use the name, trademarks, trade-names, and logos of the Company only in connection with the license granted in this Contract, but in no other connection. The Distributor may indicate, in sales or marketing media or materials, that it is an authorized distributor of the Company and of the Product. The Distributor shall not use the Company's name in either its own corporate name or any fictitious business name.

- 9.4 The Distributor shall promptly notify the Company, in writing, of any and all infringements of the Company's Intellectual Property Rights and shall assist the Company, at the Company's expense, in any action deemed necessary by the Company to protect its above mentioned rights.

- 9.5 Except as required or intended by this Contract, to maintain full and complete secrecy, not to divulge, publicize or transfer in any manner to any third party who is not a party to this Contract, and/or to make any use whatsoever of any information and/or knowledge which is connected with the Company, including information connected with the Product and/or the commercial know-how and/or any and all information regarding:

- (a) The Product Customers and potential Customers (including names, addresses, telephone and fax numbers, contact persons, dates of inquiry, prices, quantities of orders, dates of orders, etc.).
- (b) Company's market share (including any segment of such market share that shall be generated through the Distributor's services and/or through the Distributor's work-yield).
- (c) Company's marketing and/or sales policies, strategies and methods.

Furthermore, Distributor undertakes to maintain full and complete confidentiality in regard to all information connected with the Company and which is not within the public domain, including information connected with the Company's shareholders, directors and/or any other officers therein.

Article X - Term and Termination

- 10.1 The term of this Contract shall commence on the date shown at the beginning of this Contract, and shall expire on 30.04.1998.
- 10.2 Each party may terminate this Contract upon 60 days notice in writing to the other party, demanding to cure any default in performance of any obligation under this Contract, and upon failure to cure such default by the other party.

- 10.3 Notwithstanding article 10.2, the Company may terminate this Contract immediately upon the occurrence of one or more of the following circumstances:
- (a) The Distributor has become insolvent or has a receiver of its assets or property appointed.
 - (b) The Distributor makes any assignment of any of his rights under this Contract for the benefit of creditors.
 - (c) The Distributor is adjudicated a voluntary or involuntary bankruptcy.
 - (d) Distributor will not fulfill any one of the promises or contracts set forth in Annex A of this Contract.
- 10.4 Distributor's obligations and Company's rights (and limited warranty) contained in articles 3, 6.3, 7 & 9 shall survive any such termination.

Article XI - General

- 11.1 The rights of the Distributor under this Contract are restricted solely to the Distributor and shall not be assigned, transferred, subleased, sublicensed, encumbered, or subject to any security interest without the written authorization of the Company. Any attempted assignment will be void and of no effect.
- 11.2 The parties agree that this Contract is the complete and exclusive statement of the contract between the parties, which supersedes all prior contracts, oral or written, and all other communications between the parties relating to the subject matter of this Contract. No modification of this Contract shall be binding on either party unless it is in writing and signed by both parties.
- 11.3 Any waiver of any right or default hereunder shall be effective only if made in writing (through its Managing Director as to the Company), and in the instance given and shall not operate as or imply a waiver of any similar right or default on any subsequent occasion. No waiver by either party of any breach or series of breaches or defaults in performance by the other party, and no failure, refusal or neglect of either party to exercise any right, power or option given to it hereunder or to insist upon strict compliance with or performance of either party's obligations under this Contract, shall constitute a waiver of the provisions of this Contract with respect to any subsequent breach thereof or a waiver by either party of its right at any time thereafter to require exact and strict compliance with the provisions thereof.
- 11.4 Any clause, provision, or portion of this Contract found or ruled invalid, void, illegal or otherwise unenforceable under any law or by any court, arbitrator, or other proceeding, shall be amended to the extent required to render it valid, legal and enforceable, or deleted if no such amendment is feasible, and such amendment or deletion shall not effect the enforceability of the other provisions hereof.
- 11.5 The Company and the Distributor each irrevocably and unconditionally:
- (a) Submits itself in any legal action or proceeding relating to this Contract or arising out of this Contract, or any breach thereof, including, without limitation, any claim that said Contract, or any part thereof, is invalid, illegal or otherwise voidable or void, to the exclusive general jurisdiction of the courts of the State of Israel; and that this Contract, including the validity, interpretation, or performance of this Contract and any of its terms or provisions, and



the rights and obligations of the parties under this Contract shall be governed by, and construed and interpreted in and only in accordance with, the laws of the State of Israel.

(b): Consents that any such action or proceeding may be brought only in the courts of the State of Israel and waives any objection that it may now or hereafter have to the venue of any such action or proceeding in any such court or that such action or proceeding was brought in an inconvenient court and agrees not to plead or claim the same; and Agrees that service of process in any such action may be effected by mailing a copy thereof by registered or certified mail (or any substantially similar form of mail), postage prepaid, to each party.

11.6. Any notices required or permitted to be given hereunder shall be sent by prepaid registered or certified mail, return receipt requested, addressed to the other party at the addresses shown at the beginning of this Contract, and shall be deemed to have been given on the date shown on the return receipt thereof. Until either party advises the other party of a change in notice address, all notices shall be sent to the respective addresses specified herein.

11.7. Distributor undertakes, warrants and declares: (i) that there is no contract or undertaking or, to its knowledge, any law, regulation or legal prohibition that would prohibit it from fully complying with the terms of this Contract; (ii) that the provisions of this Contract and the parties undertakings contained herein comply with any and all legal requirements valid in the Territory or with respect thereto; (iii) to inform Company of all legal requirements applicable in the Territory or any part thereof, which relate to the marketing, distribution, sale or use of the Product, including, without limitation, any liability towards any third party arising therefrom; (iv) to acquire, on its own expense, any license or permission required for the marketing, distribution, sale or use of the coded and/or encrypted Products/Software.

Intending to be legally bound, the parties have executed this Contract:

Aladdin Knowledge Systems Ltd.
The Company

Signature

Yakki Margalit

Full Name

President

Title

ALADDIN
KNOWLEDGE SYSTEMS LTD.
3 SEIT OVED ST. TEL-AVIV
ISRAEL

Company Seal

Feitian Co. 北京市飞天新技术研究所
The Distributor

Signature

黄煜 (HUANG YU)

Full Name

Marketing Manager

Title

Company Seal



Annex A:

1. The Distributor hereby declares, represents, and warrants that at the commencement of this Contract, the registered capital of the Distributor is:
BEIJING FELTIAN NEW TECHNOLOGY COMPANY
2. The Distributor hereby declares, represents, and warrants that at the commencement of this Contract, the subscribed capital of the Distributor is:
北京飞田新技术有限公司
3. The Distributor hereby declares, represents, and warrants that at the commencement of this Contract, the Distributor's shareholders are:

Name	No of Shares	Ratio
------	--------------	-------

4. The Distributor hereby declares, represents, warrants, and agrees to notify, in writing, the Company on any change in the capital of the Distributor and/or any change of the Distributor's shareholders and/or any change in the ratio of shares held by the Distributor's shareholders.
It is further declared and agreed that the above-mentioned notification shall be delivered to the Company, in writing, at least 75 days prior to any change in the capital of the Distributor, and/or any change of the Distributor's shareholders, and/or any change in the ratio of shares held by the Distributor's shareholders.
5. Parties hereby declare and agree that any change in the capital of the Distributor, and/or any change of the Distributor's shareholders, and/or any change in the ratio of shares held by the Distributor's shareholders, not approved, in writing, by the Company, shall immediately grant the Company the right to terminate the Contract and end all the business relations between the Company and the Distributor.
6. It is stated, declared, and agreed that the Distributor shall not have any rights to receive or claim, from the Company, any amount of money as compensation and/or indemnification due to the termination of the Contract and the business relations between the parties.

**ANNEX B****ALADDIN KNOWLEDGE SYSTEMS LTD.
DEVELOPER'S AGREEMENT AND LICENSE**

All products of Aladdin Knowledge Systems Ltd. or an affiliate ("Aladdin"), including evaluation packages, hardware, diskettes, HASP® keys and the Programmer's Guides (collectively, the "Product") and all future orders, are subject to the terms stated below. If you do not accept these terms, please return the Evaluation Package and the Programmer's Guide to us, postage prepaid, within seven days of their receipt, and we will provide you with a refund, less freight and normal handling charges.

1. License. Aladdin, the developer of the Product, grants you a personal, non-transferable, non-exclusive license to use, sublicense and resell the Product enclosed in this package upon the terms set forth herein. The software, including any upgrades thereof, shall remain Aladdin's property, subject to the terms of this Agreement. Except as permitted in Section 2 below, you may neither transfer any part of the Product or otherwise make it available to anyone else, nor may you modify, disassemble, decompile, reverse engineer, revise or enhance the Software, the HASP® key or other part of the Product or attempt to discover the Software's source code.
2. Modification of Software; Sale of HASP® keys. You may merge and link the Software into your computer programs for the sole purpose of protecting such computer programs, as described in the Programmer's Guide. You may thereafter sublicense the merged Software to distributors and end-users of your computer program pursuant to the terms of this Agreement. You may make one archival copy of the Software. You may resell to end-users, subject to the limited warranty set forth in Section 3 (c) below, any HASP® keys which Aladdin sells to you.
3. Limited Warranty. Aladdin warrants for a period of twelve (12) months after the date of delivery to you, (the "Warranty Period"), the following: (a) that the Software will perform in substantial compliance with the Programmer's Guide, provided that it is used on the computer hardware and with the operating system for which it was designed; (b) that the magnetic media on which the Software is distributed is substantially free from significant defects in materials and workmanship; and (c) that the HASP® key is substantially free from significant defects in materials and workmanship.
4. Limitation of Remedies. In the event of a breach of this warranty, Aladdin's sole obligation is to replace or repair, at Aladdin's option, any Product or component thereof, free of charge. Warranty claims must be made in writing during the Warranty Period and within seven (7) days of the observation of the defect, accompanied by evidence satisfactory to Aladdin. All Products should be returned to the HASP distributor from which they were purchased (if not purchased directly from Aladdin) and shall be shipped by the returning party with freight and insurance paid. EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY, EXPRESSED OR IMPLIED, REGARDING THE PRODUCT INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Aladdin Knowledge Systems Ltd.
15 Beit Oved St., P.O.Box 11141, Tel Aviv 61110, Israel



5. **Limit of Aladdin's Liability.** Aladdin's entire liability for damages to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of Product that caused the damages or that are the subject matter of, or are directly related to, the cause of action. In no event will Aladdin be liable for any damages caused by your failure to perform your obligations, or for any loss of data, profits, savings, or any other consequential and incidental damages, even if Aladdin has been advised of the possibility of damages, or for any claims by you based on any third-party claim.
6. **Governing Law & Jurisdiction:** This Agreement is governed only by the laws of the State of Illinois and only the courts in Illinois shall have jurisdiction in any conflict or dispute arising out of this Agreement.
7. **Termination.** Your failure to comply with the terms of this Agreement shall terminate your license and this Agreement. Sections 3, 4 and 5 shall survive any termination of this Agreement.

Aladdin Knowledge Systems Ltd.
15 Beit Oved St., P.O.Box 11141, Tel Aviv 61110, Israel



MacHASP™ Price List (Macintosh)

Distributor C5, April 1997

Product	Developers Kit	Batches of 2-99	Batches of 100-199	Batches of 200-999	Batches of 1000+
MacHASP-S		16.75	15.50	15.00	14.25
MacHASP-M	19.00	19.50	18.50	17.50	16.25
MacHASP-M8		22.50	21.50	20.00	18.75
Net-MacHASP-5		43.00	40.00	35.00	
Net-MacHASP-10	35.00	53.00	50.00	48.00	
Net-MacHASP-20		65.00	62.00	59.00	
Net-MacHASP-50		80.00	76.00	73.00	
Net-MacHASP-100		100.00	90.00	81.00	
Net-MacHASP-Unlim.		190.00	180.00	170.00	

109,0497

NOTES:

- The first price-break for Net-MacHASP units is for quantities of 50-99 units; the second price-break is for over 100 units.
- Minimum Batch Size:
 - MacHASP: 2 units.
 - Net-MacHASPs: 1 unit.
- Minimum total order size: 100 units.
- The quantity discounts are for orders of Batches of the same code.
- Prices are quoted in \$US, FOB Israel.
- Prices may be changed without prior notice.

15 Beit Ovèd Street, P.O. Box 11141, Tel Aviv 61110, Israel
 Tel: 972-3-636 2222, Fax: 972-3-537 5796, E-mail: sales@aks.com, WWW: http://www.aks.com



= Annex C =

HASP® Price List (PC)

Distributor C5, April 1997

Product	Developers Kit	Batches of 2-99	Batches of 100-199	Batches of 200-999	Batches of 1000+
HASP-3		10.80	10.20	9.60	9.00
MemoHASP-1	12.00	13.20	11.60	10.80	10.00
MemoHASP-4		21.75	19.00	17.25	16.50
TimeHASP	19.00	22.75	21.00	19.00	18.55
TimeHASP-4		24.75	23.00	21.00	20.55
NetHASP-5		27.00	24.00	21.00	
NetHASP-10	25.00	42.00	40.00	38.00	
NetHASP-20		52.00	50.00	48.00	
NetHASP-50		62.00	60.00	58.00	
NetHASP-100		82.00	78.00	75.00	
NetHASP-Unlimited		162.00	152.00	147.00	
SerialHASP-M	15.00	18.00	17.00	16.00	15.25
PC-Card-HASP	35.00	41.50	38.50	36.00	33.50
AladdinCARD		21.00	19.25	19.25	19.25

NOTES:

- HASP-3, MemoHASP, and NetHASP are available in plug-in expansion-board versions (HASP-Card), for an additional \$US 12.00 over the standard price.
- The first price-break for NetHASP units is for quantities of 50-99 units; the second price-break is for over 100 units.
- AladdinCARD: Can be ordered in Standard packaging (each card individually packaged in a box), or in Bulk packaging (each card wrapped in nylon).
- Minimum Batch Size:
 - HASPs for stand-alone PCs: 2 units.
 - NetHASPs: 1 unit.
- Minimum total order size: 100 units.
- The quantity discounts are for orders of Batches of the same code.
- Prices are quoted in \$US, FOB Israel.
- Prices may be changed without prior notice.

15-Belt Oved Street, P.O. Box 11141, Tel Aviv 61110, Israel
 Tel: 972-3-636 2222, Fax: 972-3-537 5796, E-mail: sales@aks.com, WWW: http://www.aks.com



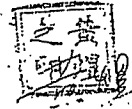
HASP36™ Price List (Japanese NEC)

Distributor C5, April 1997

Product	Developers Kit	Batches of 2-99	Batches of 100-199	Batches of 200-999	Batches of 1000+
HASP36		21.50	20.00	17.50	16.50
MemoHASP36-1	21.00	25.50	23.50	22.00	19.00
MemoHASP36-4		28.50	26.50	24.00	21.50
Net-HASP36-5		52.00	47.00	42.00	
Net-HASP36-10	35.00	71.00	65.00	58.00	
Net-HASP36-20		82.00	75.00	68.00	
Net-HASP36-50		100.00	90.00	82.00	
Net-HASP36-100		119.00	108.00	98.00	
Net-HASP36-Unlim.		237.00	208.00	189.00	

NOTES:

- The first price-break for Net-HASP36 units is for quantities of 50-99 units; the second price-break is for over 100 units.
- Minimum Batch Size:
 - HASP36 for stand-alone PCs: 2 units.
 - Net-HASP36s: 1 unit.
- Minimum total order size: 100 units.
- The quantity discounts are for orders of Batches of the same code.
- Prices are quoted in \$US, FOB Israel.
- Prices may be changed without prior notice.



OpenHASP™ Price List

Distributor C5, April 1997

Product	Developers Kit	Orders of 2-99	Orders of 100-199	Orders of 200-999	Orders of 1000+
OpenHASP	25.00	52.00	44.00	40.00	36.00
OpenHASP Master		27.00			

109,0497

NOTES:

- With the OpenHASP system, the developer assigns the code to each OpenHASP key. OpenHASP keys are sold in quantities and not in batches.
- Minimum Batch Size:
 - OpenHASP: 2 units.
 - OpenHASP Master: 1 unit.
- Prices are quoted in \$US, FOB Israel.
- Prices may be changed without prior notice.

15 Beit Oved Street, P.O. Box 11141, Tel Aviv 61110, Israel
Tel: 972-3-636 2222, Fax: 972-3-537 5796, E-mail: sales@aks.com, WWW: http://www.aks.com

Zaid Ibrahim & Co
Level 19 Menara Milenium
Pusat Bandar Damansara
50490 Kuala Lumpur
Malaysia

General 603 2087 9999
Fax 603 2094 4888
603 2094 4666

Your reference: Please advise
Our reference: SERVICE/EJ

14 April 2005

BY HAND

Softkey E-Solution Sdn Bhd
5-20 Menara KLH Business Centre
Lebuhraya Damansara Puchong
Selangor Darul Ehsan

Dear Sirs

United States District Court District of Delaware
Summons In A Civil Case Case No: 1:05-cv-00149-UNA
Aladdin Knowledge Systems, Ltd. ..Plaintiff
Feitian Technologies, Co, Ltd. Et al., .. Defendant

We have been instructed by Aladdin Knowledge Systems, Ltd. to serve the following documents on you :-

- (1) Summons in a Civil Case dated 16 March 2005;
- (2) Civil Cover Sheet; and
- (3) Complaint dated 11 March 2005 together with exhibits.

Enclosed are the abovementioned documents by way of service on you.

Please acknowledge receipt.

Yours faithfully
ZAID IBRAHIM & CO

Eugene Jayaraj
Partner

Encl

[kmy]

I/We acknowledge receipt
Of this letter and the contents
therein/the documents therein

14/4/2005

12:35 PM

Partners

- Datuk Mohd. Zaid Ibrahim
 - Chew Seng Kok
 - Loh Wei Lian
 - Lim Kar Han
 - Dato' Dr Nik Norzrul Thani
 - Kelvin Ng Hock Heng
 - Lynette Yeow
 - Paul Subramaniam
 - Mohamed Ridza
 - Wan Marzimin
 - Robert Liew
 - Toh Beng Suan
 - Tee Joe Lei
 - Lilian Liew
 - Peh Lee Kheng
 - Thavalingam Thavarajah
 - June Khoo
 - Izhar Ismail
 - Chin Sook Kwan
 - Nazlan Ghazali
 - Richard Imran Ding
 - Lim Yean Nyok
 - Mohd Azura Nik
 - Mohamed Nasri
 - Rueben Mathiavararam
 - Ariff Rozhan
 - James Patrick Monteiro
 - Eugene Jayaraj
 - Sharon Tan
 - Faizal Razak
- Johor Bahru
- Hoon Joong High
 - Dr. Clarence Edwin
 - Ng Kian Pin
- Penang
- Lena Leong
 - Ang Siak Keng
 - Khoo Kay Ping

Consultant

- Jenny Lye

SOFTKEY E-SOLUTION SDN BHD

(540674-M)
5-20, Menara KLH Business Centre,
LDP, 47100 Puchong, Selangor, Malaysia.
Tel: +603-8076 6225 Fax: +603-8070 4225

14/4/2005

12:35 PM